#2/7-19-01 V. Jones

500.39507X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): MARUKAWA

Serial No.:

Filed: January 16, 2001

Title: METHOD AND APPARATUS FOR SECURE DATA TRANSMISSION VIA NETWORK

Group:

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

January 16, 2001

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on Japanese Patent Application No.(s) 2000-013894 filed January 18, 2000.

A certified copy of said Japanese Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundidge
Registration No. 29,621

CIB/mdt
Attachment
(703)312-6600

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　１月１８日

出願番号
Application Number: 特願２０００－０１３８９４

出願人
Applicant (s): 株式会社日立製作所

２０００年１２月　１日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０９９７０８

〔書類名〕　特許願
〔整理番号〕　H99023151A
〔提出日〕　平成12年 1月18日
〔あて先〕　特許庁長官　殿
〔国際特許分類〕　H04L 9/00
H04L 12/00
〔発明者〕
〔住所又は居所〕　東京都国分寺市東恋ケ窪一丁目２８０番地
株式会社日立製作所中央研究所内
〔氏名〕　丸川　勝美
〔特許出願人〕
〔識別番号〕　000005108
〔氏名又は名称〕　株式会社日立製作所
〔代理人〕
〔識別番号〕　100075096
〔弁理士〕
〔氏名又は名称〕　作田　康夫
〔電話番号〕　03-3212-1111
〔手数料の表示〕
〔予納台帳番号〕　013088
〔納付金額〕　21,000円
〔提出物件の目録〕
〔物件名〕　明細書　1
〔物件名〕　図面　1
〔物件名〕　要約書　1
〔プルーフの要否〕　要

【書類名】　明細書

【発明の名称】　データ伝送方法

【特許請求の範囲】

【請求項１】

記載のある紙をスキャンニングおよびその後の加工処理により得たイメージをネットワークを介して電子的にやり取りするデータ伝送方法において、

データ伝送側で、

原イメージを加工処理する方法１と、上記原イメージに対してデジタル署名を適用する方法２を有し、方法１で得た加工データと方法２で得た署名データをマージし、上記マージしたデータに一方向性関数を適用し、上記一方向性関数の出力をデータ伝送側の秘密鍵で暗号化して署名データSBを得る方法３と、方法２で得た署名データをデータ受け取り側の公開鍵で暗号化して暗号化署名データSAEを得る方法４と、加工データDBと署名データSBと暗号化署名データSAEを受け取り側にデータ伝送する方法５と、

データ受け取り側で、入手した暗号化署名データSAEを，受け取り側の秘密鍵で復号化して署名データSAを得、入手した加工データDBと該署名データSAをマージして該マージしたデータに一方向性関数を適用する方法６と、入手した署名データSBをデータ伝送側の公開鍵で復号化する方法７と、方法６と方法７の結果を比較してデータに関する正当性を確認する方法８と、を持ったことを特徴とするデータ伝送方法。

【請求項２】

記載のある紙をスキャンニングおよびその後の加工処理により得たイメージをネットワークを介して電子的にやり取りするデータ伝送方法において、

データ伝送側で，原イメージに対してデジタル署名を適用する方法２を有し、原イメージと方法２で得た署名データをマージして該マージしたデータに一方向性関数を適用し、該一方向性関数の出力をデータ伝送側の秘密鍵で暗号化して署名データSBを得る方法３と、方法２で得た署名データをデータ受け取り側の公開鍵で暗号化して暗号化署名データSAEを得る方法４と、原イメージDBと署名データSBと暗号化署名データSAEを受け取り側にデータ伝送する方法５と、

データ受け取り側で，入手した暗号化署名データSAEを受け取り側の秘密鍵で復号化し、署名データSAを得、入手した原イメージDBと該署名データSAをマージして該マージしたデータに一方向性関数を適用する方法６と、入手した署名データSBを，データ伝送側の公開鍵で復号化する方法７と、方法６と方法７の結果を比較してデータに関する正当性を確認する方法８と、を持ったことを特徴とするデータ伝送方法。

【請求項３】

請求項１もしくは請求項２の方法２で得た署名データの代用として，原イメージにかかわるデータを用いたことを特徴とするデータ伝送方法。

【請求項４】

請求項１もしくは請求項２の方法６と方法７の結果を比較して、該結果が異なる場合，

データ受け取り側で、入手した暗号化署名データSAEを受け取り側の秘密鍵で復号化し署名データSAを得、該署名データSAをデータ伝送側に送付する方法と、

データ伝送側で、請求項１もしくは請求項２の方法２で生成した署名データ、もしくは請求項３の原イメージ関わるデータが送付された署名データSAと等しくなる原イメージを探索する方法、を持ったことを特徴とするデータ伝送方法。

【請求項５】

電子画像イメージ（原画像）と第１の秘密鍵を入力し、該第１の秘密鍵を用いて該電子画像イメージを暗号化し、該暗号化により、第１のデジタル署名を得て、該電子画像イメージと該第１のデジタル署名とを出力する第１の暗号化手段と、

上記電子画像イメージを入力して、該電子画像イメージの部分イメージ又は加工イメージを出力する加工処理手段と、

上記部分イメージまたは上記加工イメージと、上記第１のデジタル署名と、第２の秘密鍵を入力し、該部分イメージまたは該加工イメージと該第１のデジタル署名と該第２の秘密鍵とを用いて、該部分イメージ又は該加工イメージを暗号化して出力する第２の暗号化手段と、

上記暗号化された情報を外部の伝送路へ送信する送信手段と、を有するデータ

伝送装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は，帳票，伝票，申込書などをスキャンニングして得たイメージをネットワークを介して電子的にやり取りする際、原イメージや，原イメージから加工して生成した部分イメージなどの加工データを伝送する際のセキュリティに係わる。特に、成り済ましによる原イメージや加工データの改ざんの検証、と同時に、加工データが原イメージから生成されたかどうかを検証し、原ｲﾒｰｼﾞが改ざんされていると判定された場合には原イメージを容易に発見する方法に関する。

【０００２】

【従来の技術】

本発明に関連する従来の技術には、辻井，笠原：暗号と情報セキュリティ、昭晃堂（1999）に書かれているようなデジタル署名が知られている。この技術を用いると、図７に示すようなネットワーク1010で結ばれたA支店1000と処理センター1005間でデータ伝送を行う場合に、データを受け取った側が受け取ったデータが正規の送信側から伝送されたことを検証することができ、また送られたデータが改ざんされていないことを検証することができる。これは、伝送側が生成した秘密鍵と公開鍵を利用した公開鍵暗号により実現される。

【０００３】

デジタル署名を利用したデータ伝送の処理フローの例を図２（a）に示す。伝送する対象データDAを入手し（ステップ200）、DAにハッシュ関数を適用し（ステップ205）、ハッシュ関数出力に対し、データ伝送側の秘密鍵KEAを用いた暗号化を行い署名データSAを作成し（ステップ210）、SAを受信側に伝送する（ステップ215）。また、伝送されたデータに関して正当性の検証の処理フローの例を図２（b）に示す。対象データDAと署名データSAを入手し（ステップ220）、DAにハッシュ関数を適用し（ステップ225）、そして署名データSAに対し、予め配付された公開鍵KDAを用いた復号化を行い（ステップ230）、そしてステップ225とステップ230の結果を比較し（ステップ235）、その結果によりデータに関しての

正当性を確認する（ステップ240）。ここで，比較したデータが等しければ不正行為はなく、等しくなければ何らかの不正行為があったと推測される。

【０００４】

しかしながら、上記のことが行えると同時に、加工したデータに対し、それが原イメージから生成されたものであるかどうかを検証し、改ざんされている場合に原イメージを発見する方法はない。

【０００５】

【発明が解決しようとする課題】

膨大な量の帳票、伝票、申込書などを扱う官公庁や民間企業においては、紙メディアから電子メディアを利用し、また分散したセンターや支店をネットワークで結んで電子メディアを利用して、業務の迅速化を計りたいと言ったニーズがある。これを実現するため、紙メディアをイメージに変換し、これをワークフローに適用した業務形態が現れ始めている。そこでは、業務に必要な部分イメージなどの加工データがデータ伝送の効率化などを理由に扱われる。図６に示すの医療・保険関係の書類の部分的なイメージのように，原イメージ中の必要な部分イメージ、例えば、整理番号、診療月、医療コード、部屋番号、生年月日等を切出し、図７のネットワーク1010を介し、A支店1000から処理センター1005に伝送する。原イメージ全体を伝送したのではデータ量が大きく、また原イメージを表示したのではプライバシーに関わる情報が漏えいするおそれがあるため、必要な部分のイメージを切出し、支店Aから処理センターに伝送し、部分イメージを表示し、これを見ながらデータ入力業務を行う。

【０００６】

しかしながら、ネットワークを使いデータ伝送を行う場合、ネットワーク上を流れる原イメージや加工データが盗聴され、原イメージや加工データの一部あるいは全部が不当に改ざんされ、成り済ましにより不当な業務を行うと言った問題を防ぐことが望まれており、上記のことを回避するためには、成り済ましによる改ざんの不正行為を検証する必要がある。

【０００７】

その検証方法として、公開鍵暗号に基づくデジタル署名が知られている。しかし

，原イメージや加工データ自体が盗聴され、またイメージ入力部や加工データ処理部で扱う秘密鍵が盗まれた場合、盗聴者は容易に原イメージや加工データを改ざんし、成り済ましてデータを伝送側に送り、データの受け側では不正行為を検出できず、不当な処理を行ってしまうと言った問題が生じる。

【０００８】

本発明の第１の目的は、原イメージや加工データが盗聴され、またデータ入力部や加工データ処理部で扱う秘密鍵が盗まれた場合、盗聴者が改ざんした原イメージや加工データを成り済ましてデータ伝送されても、データの受け取り側でその不正行為を検証する方法を提供することである。

【０００９】

また、伝送したデータが改ざんされた場合、改ざんされた原イメージを早期に発見し必要な情報を再抽出する必要がある。

【００１０】

本発明の第２の目的は、データの受け取り側で、加工したデータに対し、それが原イメージから生成されたものであるかどうかを検証し、改ざんされたイメージであることを発見した場合には、原イメージを早期に入手する方法を提供することである。

【００１１】

【課題を解決するための手段】

上記の目的を達成するため、本発明は次の構成とする。

【００１２】

第１の構成として、データ伝送側で、

原イメージを加工処理して得た加工データと，原イメージに対してデジタル署名を適用して得た署名データをマージし、該マージしたデータに一方向性関数を適用し、該一方向性関数の出力をデータ伝送側の秘密鍵で暗号化し、署名データSBを得る。そして、原イメージに対し、デジタル署名を適用して得た署名データをデータ受け取り側の公開鍵で暗号化し、暗号化署名データSAEを得る。そして、加工データDBと署名データSBと暗号化署名データSAEを受け取り側にデータ伝送する。

〔００１３〕

また、データ受け取り側で、

入手した暗号化署名データSAEを受け取り側の秘密鍵で復号化し、署名データSAを得、入手した加工データDBと該署名データSAをマージし、該マージしたデータに一方向性関数を適用する。そして、入手した署名データSBをデータ伝送側の公開鍵で復号化する、そして、先に、加工データDBと該署名データSAをマージし、該マージしたデータに一方向性関数を適用した出力と、データ伝送側の公開鍵で署名データSBを復号化した結果を比較し、データに関する正当性を確認する。

〔００１４〕

第２の構成として、データ伝送側で、

原イメージと、原イメージに対してデジタル署名を適用して得た署名データをマージし、該マージしたデータに一方向性関数を適用し、該一方向性関数の出力をデータ伝送側の秘密鍵で暗号化し、署名データSBを得る。そして，原イメージに対してデジタル署名を適用して得た署名データをデータ受け取り側の公開鍵で暗号化し、暗号化署名データSAEを得る。そして、原イメージDBと署名データSBと暗号化署名データSAEを受け取り側にデータ伝送する。

〔００１５〕

また、データ受け取り側で、

入手した暗号化署名データSAEを受け取り側の秘密鍵で復号化し、署名データSAを得、入手した原イメージDBと該署名データSAをマージし、該マージしたデータに一方向性関数を適用する。そして、入手した署名データSBをデータ伝送側の公開鍵で復号化する。そして、先に、原イメージDBと該署名データSAをマージし、該マージしたデータに一方向性関数を適用した出力と、データ伝送側の公開鍵で署名データSBを復号化して得た結果を比較し、データに関する正当性を確認する。

〔００１６〕

第３の構成として、

第１の構成もしくは第２の構成において、第１の構成もしくは第２の構成の原イメージに対してデジタル署名を適用して得た署名データの代用として、原イメー

ジに係わるデータを用いる。

〔００１７〕

第４の構成として、

第１の構成もしくは第２の構成において、第１の構成もしくは第２の構成のマージしたデータに一方向性関数を適用した出力と、データ伝送側の公開鍵で署名データSBを復号化して得た結果を比較して、異なった場合、

データ受け取り側で、

入手した暗号化署名データSAEを，受け取り側の秘密鍵で復号化し署名データSAを得、該署名データSAをデータ伝送側に送付する。

〔００１８〕

また、データ伝送側で、

第１の構成もしくは第２の構成の原イメージに対してデジタル署名を適用して生成した署名データ、もしくは第３の構成の原イメージ関わるデータが送付された署名データSAと等しくなる原イメージを探索する。

〔００１９〕

また、第５の構成として、電子画像イメージ（原画像）と第１の秘密鍵を入力し、該第１の秘密鍵を用いて該電子画像イメージを暗号化し、該暗号化により、第１のデジタル署名を得て、該電子画像イメージと該第１のデジタル署名とを出力する第１の暗号化手段と、上記電子画像イメージを入力して、該電子画像イメージの部分イメージ又は加工イメージを出力する加工処理手段と、上記部分イメージまたは上記加工イメージと、上記第１のデジタル署名と、第２の秘密鍵を入力し、該部分イメージまたは該加工イメージと該第１のデジタル署名と該第２の秘密鍵とを用いて、該部分イメージ又は該加工イメージを暗号化して出力する第２の暗号化手段と、上記暗号化された情報を外部の伝送路へ送信する送信手段と、を有するデータ伝送装置とする。

〔００２０〕

【発明の実施の形態】

本発明は公開鍵暗号に基づくデジタル署名を利用する。その原理を図５と図１を用いて説明する。データの大きな流れは、支店780のイメージ入力業務700によ

り原イメージ720を得、加工処理業務705で原イメージを加工する。そして、加工したデータ730をネットワーク750、715を介して処理センター710の業務処理に伝送し、業務を行う。この流れの中で、ネットワーク上で盗聴が行われ、イメージ入力や加工処理で扱われる秘密鍵が盗まれると、成り済ましによるデータの改ざんと言った問題が生じる。

【００２１】

次に、原理を説明するために、扱うデータについて説明する。720は原イメージ、725はイメージ入力業務での秘密鍵を利用しデジタル署名により得られた署名データ、730は加工処理業務で加工した加工データ、735は725の署名データ、740は730と735を用いて一つのマージデータとし、加工処理業務での秘密鍵を利用しデジタル署名により得られた署名データ、745は処理センター710の業務処理での公開鍵により署名データ735を暗号化したデータ、755は処理センター710に伝送するデータ群で730、745、740からなる。また、760は755をネットワーク750上で盗聴し、730を改ざんしたしたデータ765、そして765と745を用いて一つのマージデータとし、加工処理業務から盗んだ秘密鍵を利用しデジタル署名により得られた署名データ770である。775は処理センター710が受け取る改ざんされ成り済まして送られたデータである。

【００２２】

従来、730の加工データと加工処理業務の秘密鍵を利用しデジタル署名により得られた署名データを利用するので、加工処理業務の秘密鍵を盗んだ盗聴者は容易に加工データを改ざんし、その署名データを作成し、それらを加工処理部に成り済まして処理センターに伝送することができ、データ受け取り側はその不正行為を検証することができない。

【００２３】

図１（a）は図５におけるデータ伝送側で行う処理フローである。原イメージである対象データDAと署名データSAと加工情報を入手する（ステップ100）。ここで、加工情報とは例えば部分イメージを扱う場合、扱う部分領域の座標などである。そして、DAと加工情報を用いた加工処理を行い（ステップ105）、データ受け取り側の業務処理の公開鍵KDCを用いて署名データSAを暗号化し暗号化署名

データSAEを得（ステップ110）、次に加工データDBと署名データSAを一つのデータになるようマージ処理し（ステップ115），マージ処理したデータDCにハッシュ関数を適用し（ステップ120）、加工処理部の秘密鍵を用いてハッシュ関数の出力を暗号化し署名データSBを得（ステップ125）、データ受け取り側にDB、SB、SAEを伝送する。ここで、DBが図５の730であり、SBが740であり、SAEが745である。

〔００２４〕

また、図１（b）は図５におけるデータ受け取り側で行う処理フローである。ここでは、受け取った加工データDBと署名データSBと暗号化署名データSAEを入手し（ステップ135）、暗号化署名データSAEを受け取り側の業務処理部の秘密鍵KECを用いて複合化しSAを得る（ステップ140）。そして、DBとSAを一つのデータとしてマージ処理し（ステップ145）、マージ処理したDCにハッシュ関数を適用し（ステップ150）、また加工処理部の公開鍵KDBを用いて署名データSBを複合化し（ステップ155）、ステップ150とステップ155の結果を比較し（ステップ160）、その結果により不正行為が行われたか否かを知ることができる。

〔００２５〕

この処理でのポイントはSAEを復号化できるのはその秘密鍵を持っているデータ受け取り側であるということであり、盗聴者がデータをいくら改ざんしまた改ざんデータと暗号化署名データを用いて署名データを作り直しても、ステップ160の結果が等しくなることはありえない。また、この流れからもわかるように暗号化署名データは必ずしも原イメージの署名データである必要はなく、原イメージに係わる情報などでよい。また，原イメージに対しても、任意のデータがあれば、加工データで扱ったように、盗聴者からの攻撃を防ぐことができる。

〔００２６〕

加工データが原イメージから生成されかどうかの検証は、図1（b）のステップ150、155を比較することにより、双方の値が等しければ、盗聴による不正はなく、加工データは原イメージから生成されたものとわかる。また、双方の値が異なれば、データの改ざんが行われている可能性があり、この場合には改ざんデータから原イメージのIDを知ることができない場合が考えられる。その場合、伝送さ

れた暗号署名データをデータ受け取り側から複合化し、データ転送側に送付してもらい、これと一致するデータ転送側の原イメージの署名データを探索することで、原イメージを発見できる。

【００２７】

次の実施例として、実際に、複数個の部分イメージを生成する加工処理に関係する場合の処理について、図３を用いて説明する。

【００２８】

この場合、ステップ300からステップ310は、図1（a）のステップ100からステップ110と同じであり、ステップ315以下のステップ320からステップ335の処理は各部分イメージに対し行うもので、図1（a）のステップ115からステップ130と同じであり、異なるのはステップ315が加工データ数回繰り返し処理を実行させる点である。

【００２９】

また、図4は図３の処理に対応するフローであり、伝送されたデータに関し検証を行う処理フローである。これもデータ伝送側と同じように、図4のステップ400からステップ405は、図1（b）のステップ135からステップ140と同じであり、ステップ410以下のステップ415からステップ435の処理は各部分イメージに対し行うもので、図1（b）のステップ145からステップ165と同じであり、異なるのはステップ410が加工データ数回繰り返し処理を実行させる点である。

【００３０】

したがって、部分イメージを抽出し、盗聴による不正行為を行うことなく、それらデータをデータ受け取り側に伝送でき、盗聴による不正行為を検証できる。

【００３１】

【発明の効果】

従来，デジタル署名により生成されたデータがネットワーク上で盗聴され、かつそこで用いた秘密鍵が盗まれた場合、盗聴者がデータを改ざんし、成り済ましてデータを伝送した結果、受け取り側で不当な処理が行われると言った問題が生じる。しかし、本発明によれば、データ受け取り側で、データの改ざんもしくは成り済ましの不正行為を検証できる。

【図面の簡単な説明】

【図１】

本発明の処理フロー。

【図２】

従来のデジタル署名の処理フロー。

【図３】

加工処理：部分イメージ処理での，データ伝送側の署名データ等のデータ生成の処理フロー。

【図４】

加工処理：部分イメージ処理での，データ受け取り側のデータ伝送者およびデータの正当性を検証する処理フロー。

【図５】

原イメージ，加工データ，署名データなどについて，データ受け取り側までの流れを示す図。

【図６】

加工処理：部分イメージ処理の利用例を示す図。

【図７】

本発明を適用するシステムの例。

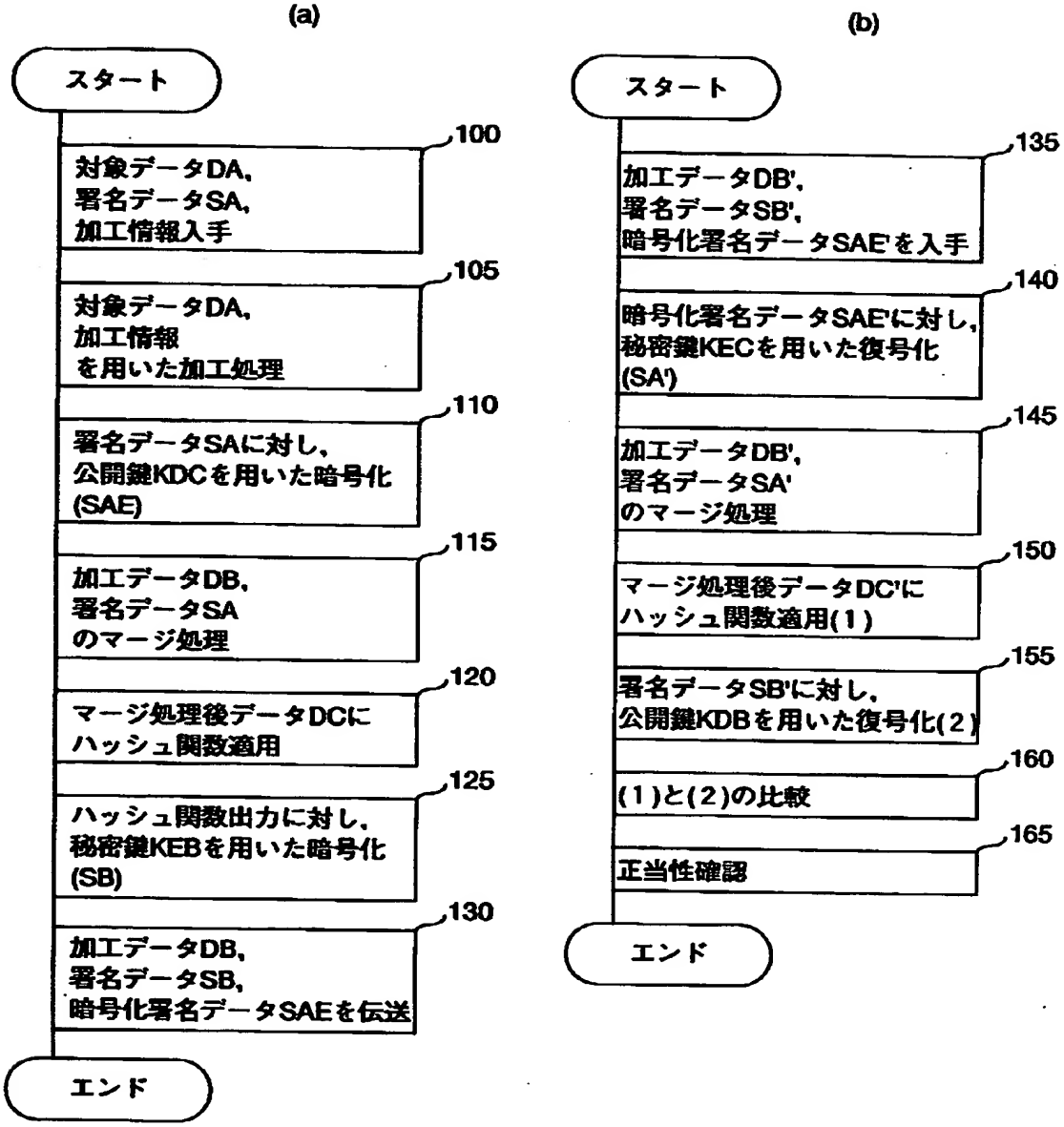
【符号の説明】

100：処理を行うためのデータを入力する部分、105：加工処理を実行する部分、110：データ受け取り側の公開鍵による署名データの暗合化、115：加工データと署名データとのマージ処理、120：マージデータにハッシュ関数の適用、125：ハッシュ関数の出力を加工処理部の秘密鍵で暗号化処理、130：生成データの伝送、135以下はデータ受け取り側での処理であり、135：伝送データの入手、140：暗号化された証明データ110の復号化、145：加工データと署名データとのマージ処理、150：マージ処理データにハッシュ関数を適用、155：署名データの複合化、160：150と155の結果比較、165：比較結果による正当性の確認。

【書類名】　図面

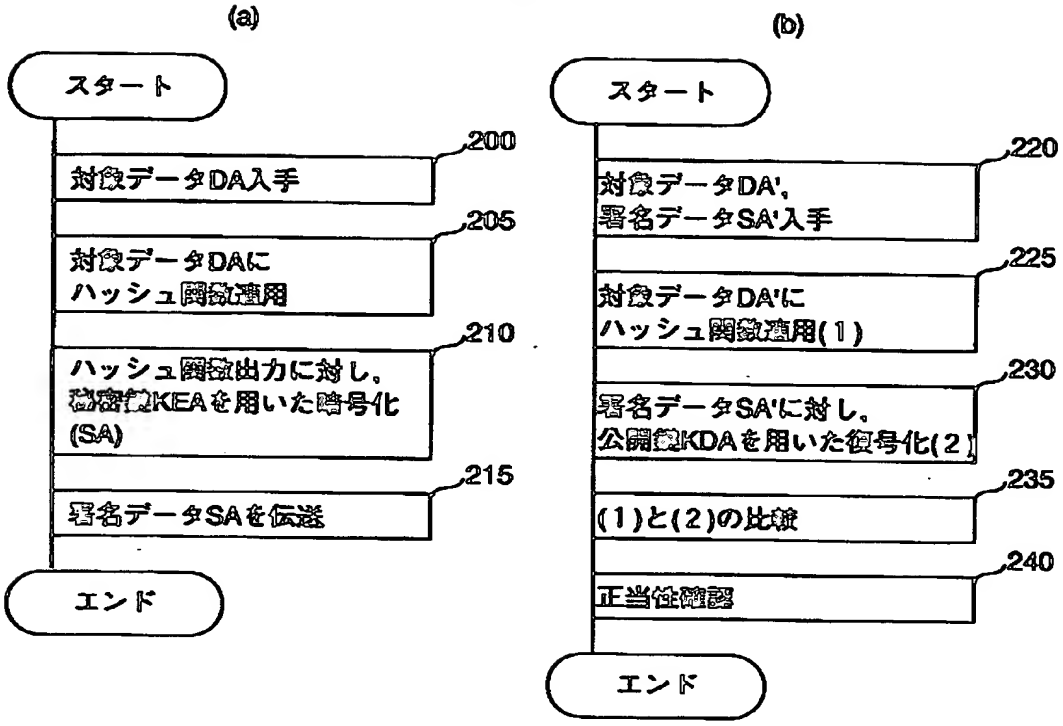
【図１】

図1


(a)
スタート
100
対象データDA,
署名データSA,
加工情報入手
105
対象データDA,
加工情報
を用いた加工処理
110
署名データSAに対し,
公開鍵KDCを用いた暗号化
(SAE)
115
加工データDB,
署名データSA
のマージ処理
120
マージ処理後データDCに
ハッシュ関数適用
125
ハッシュ関数出力に対し,
秘密鍵KEBを用いた暗号化
(SB)
130
加工データDB,
署名データSB,
暗号化署名データSAEを伝送
エンド
(b)
スタート
135
加工データDB',
署名データSB',
暗号化署名データSAE'を入手
140
暗号化署名データSAE'に対し,
秘密鍵KECを用いた復号化
(SA')
145
加工データDB',
署名データSA'
のマージ処理
150
マージ処理後データDC'に
ハッシュ関数適用(1)
155
署名データSB'に対し,
公開鍵KDBを用いた復号化(2)
160
(1)と(2)の比較
165
正当性確認
エンド

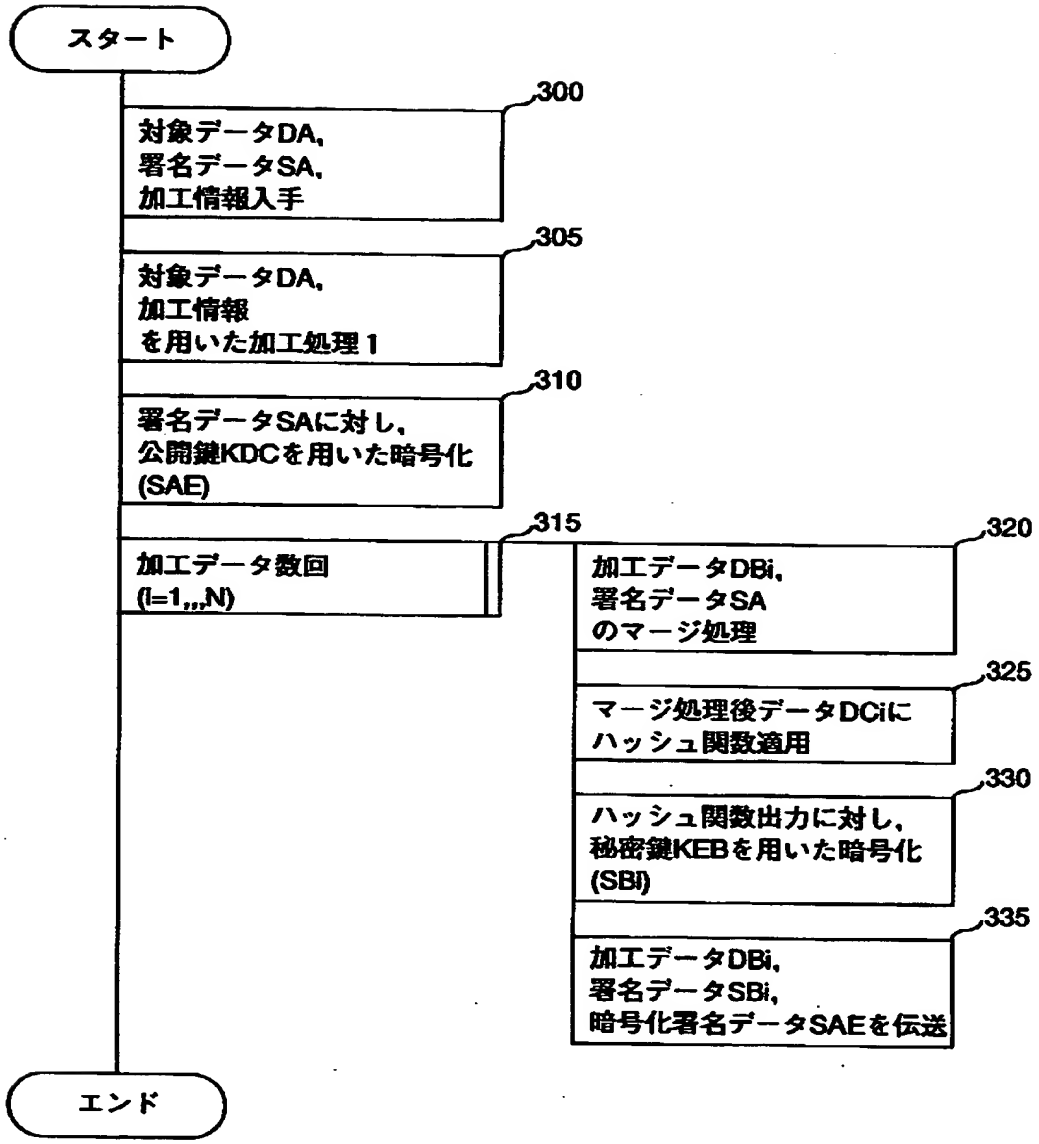
【図２】

図２


(a)
スタート
200
対象データDA入手
205
対象データDAに
ハッシュ関数適用
210
ハッシュ関数出力に対し、
秘密鍵KEAを用いた暗号化
(SA)
215
署名データSAを伝送
エンド
(b)
スタート
220
対象データDA'、
署名データSA'入手
225
対象データDA'に
ハッシュ関数適用(１)
230
署名データSA'に対し、
公開鍵KDAを用いた復号化(２)
235
(１)と(２)の比較
240
正当性確認
エンド

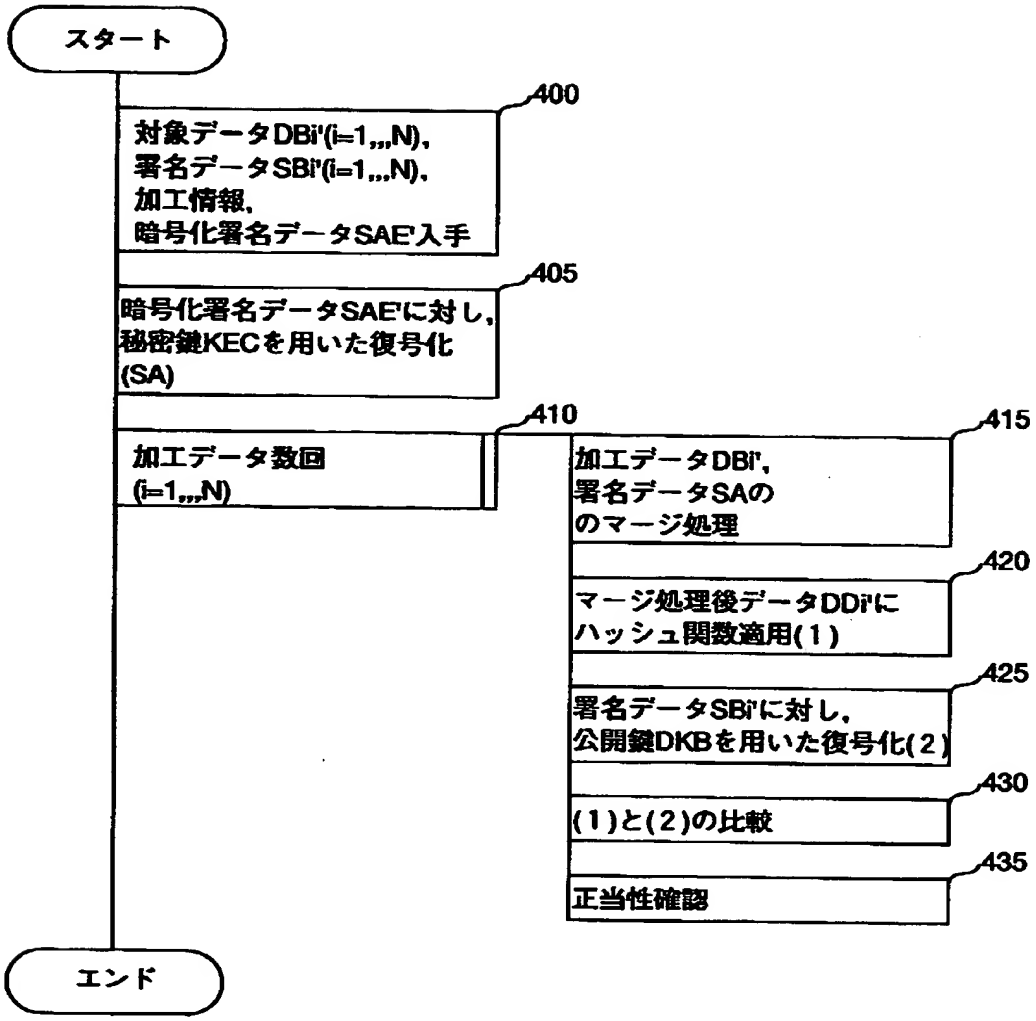
【図３】

図３


スタート
300
対象データDA、
署名データSA、
加工情報入手
305
対象データDA、
加工情報
を用いた加工処理１
310
署名データSAに対し、
公開鍵KDCを用いた暗号化
(SAE)
315
加工データ数回
(I=1,,,N)
320
加工データDBi、
署名データSA
のマージ処理
325
マージ処理後データDCiに
ハッシュ関数適用
330
ハッシュ関数出力に対し、
秘密鍵KEBを用いた暗号化
(SBI)
335
加工データDBi、
署名データSBi、
暗号化署名データSAEを伝送
エンド

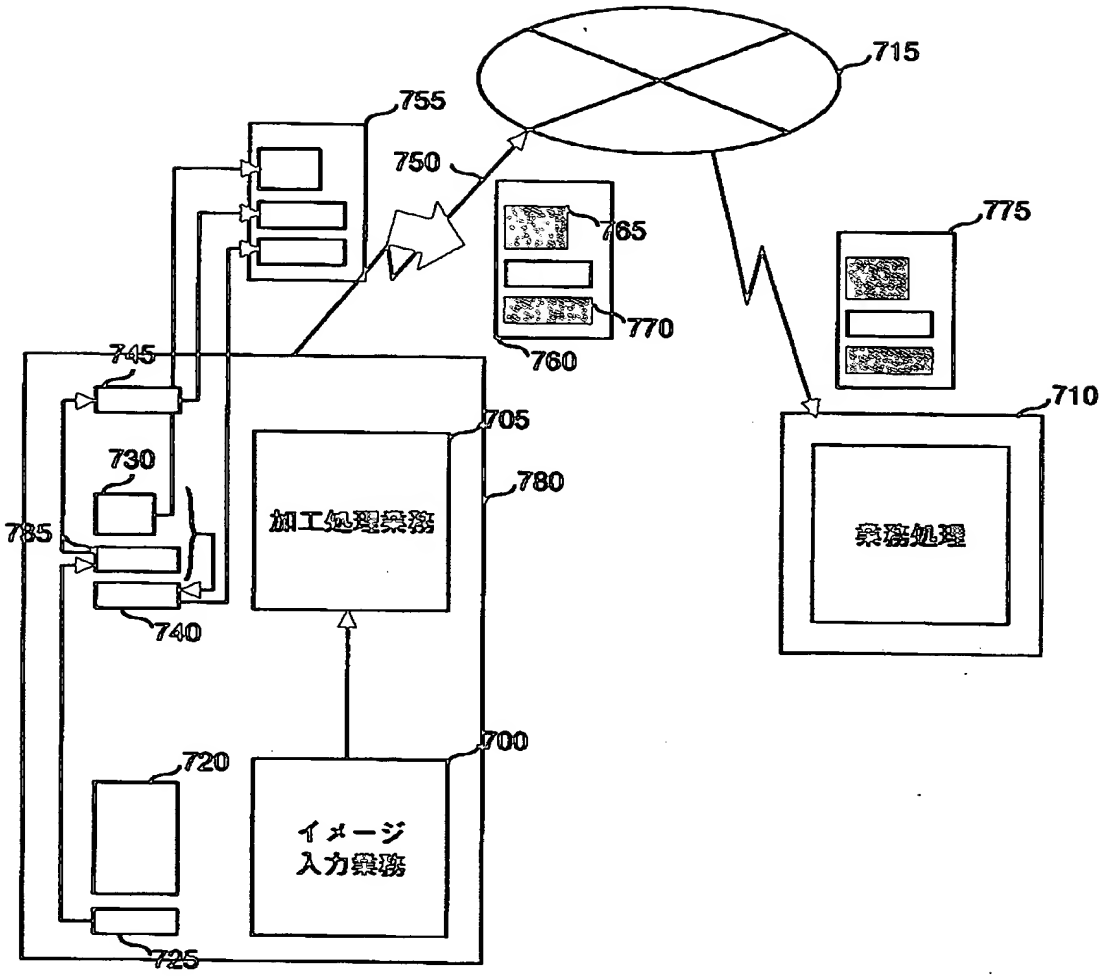
【図４】

図4


スタート
400
対象データDBi'(i=1,,,N),
署名データSBi'(i=1,,,N),
加工情報,
暗号化署名データSAE'入手
405
暗号化署名データSAE'に対し,
秘密鍵KECを用いた復号化
(SA)
410
加工データ数回
(i=1,,,N)
415
加工データDBi',
署名データSAの
のマージ処理
420
マージ処理後データDDi'に
ハッシュ関数適用(１)
425
署名データSBi'に対し,
公開鍵DKBを用いた復号化(２)
430
(１)と(２)の比較
435
正当性確認
エンド

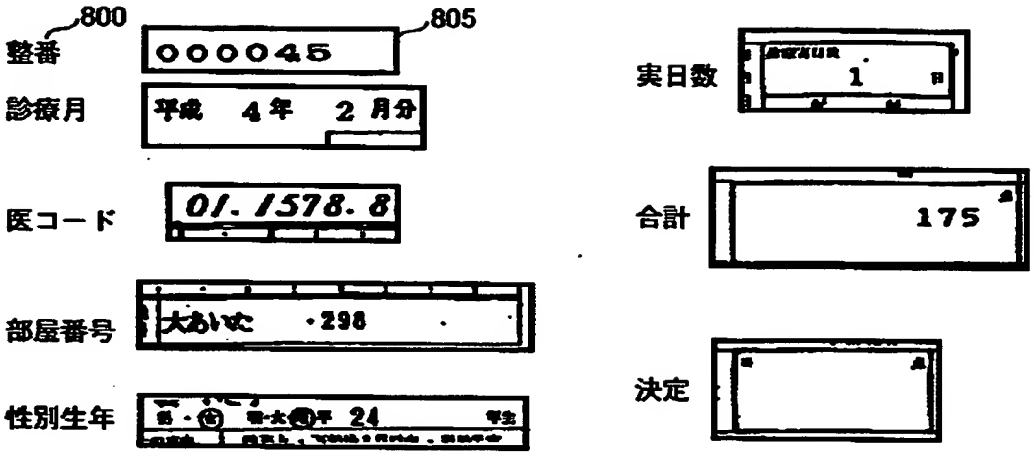
【図５】

図5


715
755
750
765
775
770
760
745
705
710
730
780
加工処理業務
業務処理
735
740
720
700
イメージ
入力業務
725

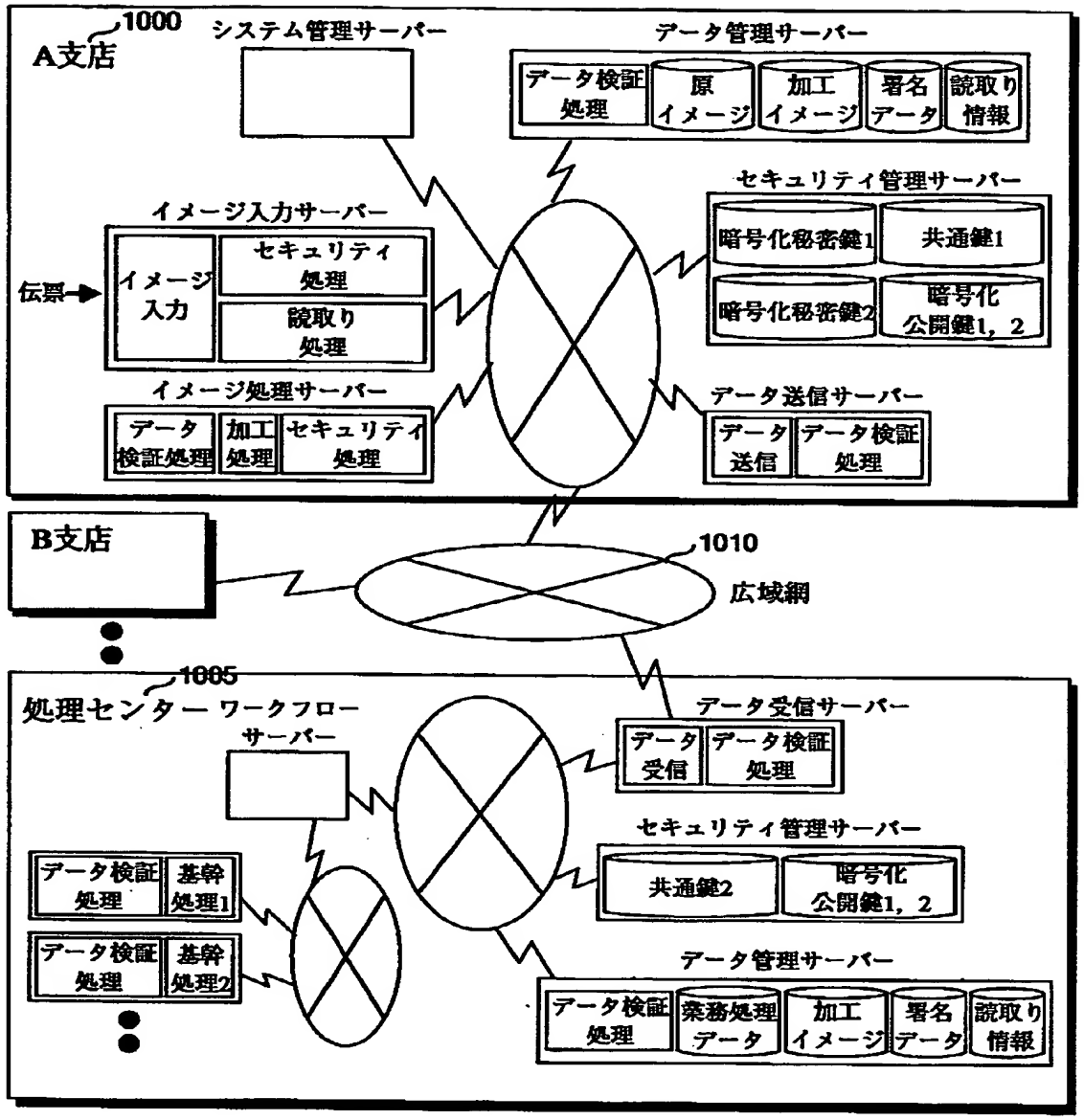
【図６】

図６


800
805
整番
000045
診療月
平成 4年 2月分
医コード
01. 1578. 8
部屋番号
大あいた ・298
性別生年
実日数
1
合計
175
決定

【図７】

図 7


1000
A支店
システム管理サーバー
データ管理サーバー
データ検証処理
原イメージ
加工イメージ
署名データ
読取り情報
セキュリティ管理サーバー
暗号化秘密鍵1
共通鍵1
暗号化秘密鍵2
暗号化公開鍵1，2
イメージ入力サーバー
伝票
イメージ入力
セキュリティ処理
読取り処理
イメージ処理サーバー
データ検証処理
加工処理
セキュリティ処理
データ送信サーバー
データ送信
データ検証処理
B支店
1010
広域網
1005
処理センター
ワークフローサーバー
データ受信サーバー
データ受信
データ検証処理
セキュリティ管理サーバー
共通鍵2
暗号化公開鍵1，2
データ検証処理
基幹処理1
データ検証処理
基幹処理2
データ管理サーバー
データ検証処理
業務処理データ
加工イメージ
署名データ
読取り情報

【書類名】　要約書

【要約】

【課題】　盗聴者が改ざんしたデータを成り済まして伝送しても，受け取り側でその不正行為、又は加工データの原票性を検証し、改ざんされた原イメージを容易に発見することを目的とする。

【解決手段】　データ伝送側から、加工データDBと、原イメージの署名データをマージして得られる出力を伝送側の秘密鍵で暗号化した署名データSBと、受け取り側の公開鍵で暗号化した原イメージの署名データSAから得た暗号化署名データSAEとを、受け取り側に伝送する。

データ受け取り側では、受け取り側の秘密鍵で復号化したSAEよりSAを得、DBとSAをマージする。SBを、データ伝送側の公開鍵で復号化する。DBとSAとのマージ出力と、SBの復号化結果を比較し、データに関する正当性を確認する。

【効果】　データの改ざんや成り済まし等の不正行為、又加工データが原票性を検証し、改ざん前の原イメージを容易に発見できる。

【選択図】　図１

出 願 人 履 歴 情 報

識別番号　〔０００００５１０８〕

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所